Web Images Video News Maps more »

Google scholar hash concatenation key generation - 2001 Searc

Search only in Engineering, Computer Science, and Mathematics.

Search in all subject areas.

Scholar **All articles** - Recent articles Results **1** - **100** of about **2,590** for **hash concatenation key ge**

UMAC: Fast and secure message authentication- ▶ fastcrypto.org [PDF]
J Black, S Halevi, H Krawczyk, T Krovetz, P ... - Advances in Cryptology–CRYPTO, 1999 - Springer
... one could **hash** the message twice, using independent **hash** keys, and **concatenate** the results. **...** keys that are used are not independent; rather, one **key** is the **...**
Cited by 182 - Related articles - Web Search - BL Direct - All 30 versions

Yarrow-160: Notes on the design and analysis of the yarrow cryptographic pseudorandom number ...- ▶ future.co.kr [PDF]
J Kelsey, B Schneier, N Ferguson - Lecture notes in computer science, 2000 - Springer
... gate, we generate a new **key** from the old **key** using a **...** Once we have collected enough entropy we apply the **hash** function h to **...** the **concatenation** of all inputs. **...**
Cited by 60 - Related articles - Web Search - BL Direct - All 20 versions

Software performance of universal **hash** functions- ▶ saitama-u.ac.jp [PDF]
W Nevelsteen, B Preneel - Lecture notes in computer science, 1999 - Springer
... bucket **hashing**, bucket **hashing** with a short **key**, fast polynomial **...** of the buckets is computed, and the **hash** function output is the **concatenation** of the **...**
Cited by 37 - Related articles - Web Search - BL Direct - All 15 versions

Robustness principles for public **key** protocols- ▶ rediris.es [PDF]
R Anderson, R Needham - Lecture Notes in Computer Science, 1995 - Springer
... then signs it with her private **key**. Denoting the modulus, public exponent and private exponent of party a by n,, e, and d,, and ignoring **hashing** (as it makes **...**
Cited by 189 - Related articles - Web Search - BL Direct - All 38 versions

Bucket hashing with a small **key** size- ▶ kfupm.edu.sa [PDF]
T Johansson - Lecture Notes in Computer Science, 1997 - Springer
... This requires the **key** to be generated through a pseudo-random number **generator**. **...** work on software effi- ciency of universal **hash** functions, [17, 24, 11 **...**
Cited by 19 - Related articles - Web Search - BL Direct - All 9 versions

[PDF] ▶ The s/**key** (tm) one-time password system
NM Haller - Symposium on Network and Distributed System Security, 1994 - lhermie.homelinux.com
... The result of the **concatenation** is passed through MD4, and **...** Because the number of **hash** function iterations executed by **...** **Generation** of S/**KEY** One-Time Passwords **...**
Cited by 457 - Related articles - View as HTML - Web Search - All 116 versions

The state of cryptographic **hash** functions- ▶ psu.edu [PDF]
B Preneel - Lecture Notes in Computer Science, 1999 - Springer
... proof systems, pseudo-random number **generation**, complexity theory **...** An -almost strongly universal **hash** function family **...** The secret **key** K chooses a function in **...**
Cited by 48 - Related articles - Web Search - BL Direct - All 14 versions

A digital multisignature scheme using bijective public-**key** cryptosystems
T Okamoto - ACM transactions on computer systems, 1988 - portal.acm.org

... Moreover, one-way **hash** functions cannot be used: thus the pro ... denotes **concatenation** ... 2.2 Procedure (1) **Key generation** and publication When each signer i (i = 1, 2 ...
Cited by 99 - Related articles - Web Search

Keying **hash** functions for message authentication- ▶ ucsd.edu [PDF]
M Bellare, R Canetti, H Krawczyk - Lecture Notes in Computer Science, 1996 - Springer
... this is broken. Page 4. problem is to **key** these **hash** functions through their initial variable (IV) (for details see Section 2). That ...
Cited by 666 - Related articles - Web Search - BL Direct - All 39 versions

Analysis of the Internet **Key** Exchange protocol using the NRLProtocol Analyzer- ▶ kfupm.edu.sa [PDF]
C Meadows - Security and Privacy, 1999. Proceedings of the 1999 IEEE ..., 1999 - ieeexplore.ieee.org
... on a specication of the Needham-Schroeder public- **key** protocol, its ... to treatatrivialalltermsencounteredof the form X,Y for **concatenation** and **hash** X for ...
Cited by 127 - Related articles - Web Search - Library Search - BL Direct - All 12 versions

Two-phase cryptographic **key** recovery system
R Gennaro, DB Johnson, PA Karger, SM Matyas Jr, M ... - US Patent 5,937,066, 1999 - Google Patents
... P, Q and (optionally) R. The session **key** is created by combining the P and Q values by XOR addition, **concatenating** the result with R, and **hashing** the concatena ...
Cited by 35 - Related articles - Web Search - All 4 versions

Public-**key** cryptography and password protocols: The multi-user case- ▶ kfupm.edu.sa [PDF]
MK Boyarsky - Proceedings of the 6th ACM conference on Computer and ..., 1999 - portal.acm.org
... assume that f is indeed the **concatenation** function. ... a universal family of one-way **hash** functions as ... **Key generation**: Run GP(n), the probabilistic encryp- tion ...
Cited by 60 - Related articles - Web Search - All 13 versions

Message encryption using a **hash** function
CW Kaufman, RJ Perlman - US Patent 5,483,598, 1996 - Google Patents
... at the receiving station includes a **hash** code **generator** 210 which receives the **concatenation** of the secret ... 210 is the random number **key** pad segment ...
Cited by 8 - Related articles - Web Search - All 2 versions

[PDF] ▶ RSA Security response to weaknesses in **key** scheduling algorithm of RC4
R Rivest - Technical note, RSA Data Security, Inc, 2001 - comms.scitech.sussex.ac.uk
... the keys is to add or **concatenate** a counter ... vector by passing them through a **hash** function such ... Alternatively, weaknesses in the **key** scheduling algorithm can ...
Cited by 9 - Related articles - View as HTML - Web Search - All 8 versions

[PDF] ▶ Efficient construction of vote-tags to allow open objection to the tally in electronic elections
A Riera, J Rifà, J Borrell - Information Processing Letters, 2000 - ccd.uab.es
... The standard for one-way **hash** functions, SHA [5 ... 8]. This means that, assuming the **concatenation** of the vote ... In contrast, **key generation** for 512-bit modulo DSA [4 ...
Cited by 12 - Related articles - View as HTML - Web Search - All 6 versions

... cryptographic **hash** functions and methods for amplifying the security of **hash** functions and pseudo- ...
WA Aiello, R Venkatesan - US Patent 5,608,801, 1997 - Google Patents
... PRF) from 2n bits to 2n bits with **key** K. The B ... n bits to n bits wherein K is the **concatenation** of eight ... sum (FFSS) **Hashing**: FFSS **hashing** is a **hash** function that ...
Cited by 18 - Related articles - Web Search - All 7 versions

GOST 34.10—A brief overview of Russia's DSA- ▶psu.edu [PDF]
M Michels, D Naccache, H Petersen - Computers & Security, 1996 - Elsevier
... the coding of the word A Vfi4(2) with **key** K V25o **... concatenation** of the words C, DB*; A is the **concatenation** of A **...** Overview The **hash** function h : B* X V256(2) V256(2 **...**
Cited by 13 - Related articles - Web Search - BL Direct - All 21 versions

Arbitration in tamper proof systems
GI Davida, BJ Matt - Proceedings Advances in Cryptology-Crypto'87, 1987 - Springer
... B user A's secret **key** and the public **key** of user B are entered into the device. **... concatenated** to the message and a cryptographic **hash ...**
Cited by 8 - Related articles - Web Search - All 2 versions

Hybrid public **key** algorithm/data encryption algorithm **key** distribution method based on control ...
SM Matyas, DB Johnson, AV Le, R Prymak, JD Wilkins ... - US Patent 5,142,578, 1992 - Google Patents
... MEANS 502 ePU(keyblk) DSIG **HASH** PRODUCTION r_fc **...** 62 60 PUb K CONTROL INFORMATION **CONCATENATION** 42 MEANS **...** implementing encryption methods and **key generation** methods **...**
Cited by 38 - Related articles - Web Search - All 5 versions

Novel authentication and **key** agreement protocol for low processingpower and systems resource ...
MI Samarakoon, B Honary - IEE Colloquium on Novel DSP Algorithms and Architectures for ..., 1999 - ieeexplore.ieee.org
... Hash Encrypt **... key** of i SCA -Plivate **key** of CA PCA -Public **key** of Certification Authority (b) Certificate Verilicaffon (a) Certificate **Generation ...**
Cited by 5 - Related articles - Web Search - BL Direct - All 2 versions

Scrambling and **key** distribution scheme for digital television
W Kanjanarin, T Amornraksa - Ninth IEEE International Conference on Networks, 2001. ..., 2001 - ieeexplore.ieee.org
... from a strong collision resistant one-way **hash** function (h **...** n/2 6. Set ML' as the **concatenation** of ML **...** with.an encryption algorithm using a scrambling **key** (K,) to **...**
Cited by 12 - Related articles - Web Search - All 3 versions

Accountable-subgroup multisignatures: extended abstract- ▶mit.edu [PDF]
S Micali, K Ohta, L Reyzin - Proceedings of the 8th ACM Conference on Computer and ..., 2001 - portal.acm.org
... adversary is now also allowed queries to H, which we will call "**hash** queries **...** The naive scheme is not secure at all if the ad- versary attacks **key generation**. **...**
Cited by 98 - Related articles - Web Search - All 19 versions

Integrated transport layer security: end-to-end security modelbetween WTLS and TLS- ▶uh.edu [PDF]
EK Kwon, YG Cho, KJ Chae - ... Networking, 2001. Proceedings. 15th International Conference ..., 2001 - ieeexplore.ieee.org
... y HMAC(K, M) : the secure **hash** expression of **...** in Figure 4. Puls(+) means **concatenation** in Table 1 **...** 163ECC-DSA **key generation** 163ECC-DSA sign **generation** I63ECC-DSA **...**
Cited by 30 - Related articles - Web Search - All 6 versions

Efficient **key** distribution for slow computing devices: achievingfast over the air activation for ...- ▶neu.edu [PDF]
C Carroll, Y Frankel, Y Tsiounis - 1998 IEEE Symposium on Security and Privacy, 1998. ..., 1998 - ieeexplore.ieee.org
... A heuristic implementation of a collision- intractable **hash** function based on **...** A-keys, the random number r is the **concatenation** of the session **key** and the **...**
Cited by 16 - Related articles - Web Search - BL Direct - All 11 versions

Hierarchical **key** assignment without public-**key** cryptography- ▶thu.edu.tw [PDF]
CH Lin - Computers & Security, 2001 - Elsevier
... based on very simple operations such as **concatenation** and one-way **hash** functions and **...** In this section, **key generation** and **key** derivation procedures for the **...**
Cited by 27 - Related articles - Web Search - All 8 versions

[PDF] ▶Analysis and design of cryptographic **hash** functions
B Preneel - 1993 - Citeseer
... xy : the **concatenation** of the binary strings **...** of how cryptographically secure **hash** functions can **... key generation** algorithm KG, that produces corresponding pairs **...**
Cited by 245 - Related articles - View as HTML - Web Search - Library Search - All 6 versions

Non-biased pseudo random number generator
MW Thomlinson, DR Simon, B Yee - US Patent 5,778,069, 1998 - Google Patents
... it is computationally infea- sible to derive the initializing **key** or seed **... generator** as recited in claim 1 lates a **hash** value of a **concatenated** version of **...**
Cited by 16 - Related articles - Web Search - All 2 versions

Min-round resettable zero-knowledge in the public-**key** model- ▶mit.edu [PDF]
S Micali, L Reyzin - Lecture Notes in Computer Science, 2001 - Springer
... time; this is easy to satisfy by simply including the random string used in **key generation** into the secret **key**. **...** 3.3 **Hash**-Based Commitment Schemes **...**
Cited by 22 - Related articles - Web Search - BL Direct - All 18 versions

" Pseudo-Random" Number **Generation** within Cryptographic Algorithms: The DSS Case
M Bellare, S Goldwasser, D Micciancio - Lecture Notes in Computer Science, 1997 - Springer
... where the k values are formed by **concatenating** 5 consecutive **...** on the DSS algorithm does not involve the **hash** function H **...** On input a secret **key** x, a seed a to the **...**
Cited by 37 - Related articles - Web Search - BL Direct - All 4 versions

System and method for generating unique secure values for digitally signing documents
N Hardy, LL Vetter, ED Tribble - US Patent 6,079,018, 2000 - Google Patents
... k. 15 Claims, 6 Drawing Sheets Digital Signature Procedure 140A 'Pseudo- I Random [**Key Gen**. Proc. **Hash** Proc -146 Document Digest combine (**concatenate**) 148 160A **...**
Cited by 5 - Related articles - Web Search - All 2 versions

Yaksha: Augmenting Kerberos with public **key** cryptography- ▶findravi.com [PDF]
R Ganesan - Network and Distributed System Security, 1995., Proceedings ..., 1995 - ieeexplore.ieee.org
... They assume that **key generation** is conducted by a trusted 3rd party, like a tamper proof chip, and the factorization of the RSA modulus and @(n) are discarded **...**
Cited by 85 - Related articles - Web Search - All 3 versions

[PDF] ▶Immunizing public **key** cryptosystems against chosen ciphertext attacks
Y Zheng, J Seberry - IEEE Journal on Selected Areas in Communications, 1993 - Citeseer
... the second on the use of universal **hash** functions, and **...** C is denoted by 1x1, and the **concatenation** of two **...** is called a **key-generation** algorithm which, on input n **...**
Cited by 56 - Related articles - View as HTML - Web Search - BL Direct - All 19 versions

Weaknesses in the **key** scheduling algorithm of RC4- ▶uninett.no [PDF]
S Fluhrer, I Mantin, A Shamir - Lecture Notes in Computer Science, 2001 - Springer
... of the 802.11 standard), in which a fixed secret **key** is **concatenated** with known **...** 1. The **Key** Scheduling Algorithm and the Pseudo-Random **Generation** Algorithm **...**
Cited by 655 - Related articles - Web Search - BL Direct - All 77 versions

Elliptic curve cryptosystems on smart cards
E Mohammed, AE Emarah, K El-Shennawy - 2001 IEEE 35th International Carnahan Conference on Security ..., 2001 - ieeexplore.ieee.org
... The **hash** of the **concatenation** of two ... Then, each party uses the following **key generation** primitive to generate the individual public and private **key** pairs. ...
Cited by 9 - Related articles - Web Search - All 4 versions

Ticket based authentication and payment protocol for mobiletelecommunications systems
BR Lee, TY Kim, SS Kang - Dependable Computing, 2001. Proceedings. 2001 Pacific Rim ..., 2001 - ieeexplore.ieee.org
... the session **key** K . U signs the **hash** value of the **concatenation** Ticket II K II ri idv II ch.data II TSv using the private signature **generation key** computed in ...
Cited by 9 - Related articles - Web Search - All 5 versions

[PDF] ▶ Implementing network security protocols based on elliptic curve cryptography
M Aydos, E Savas, CK Koc - Proceedings of the Fourth Symposium on Computer Networks, 1999 - christianroepke.de
... The **hash** of the **concatenation** of two ... Then, the following **key generation** primitive is used by each party to generate the individual public and private **key** ...
Cited by 11 - Related articles - View as HTML - Web Search - All 15 versions

Pseudorandom number generator
RS DeBellis, RM Smith Sr, PCC Yeh - US Patent 6,044,388, 2000 - Google Patents
... a secret value and passing the **concatenation** result through ... way **hash** function to generate a **hash** value from ... not shown) for encryption, **key** management, digital ...
Cited by 5 - Related articles - Web Search - All 2 versions

On end-to-end security for Bluetooth/WAP and TCP/IP networks
S Sengodan, D Smith, M Abou-Rizk, NR Center, MA ... - 2000 IEEE International Conference on Personal Wireless ..., 2000 - ieeexplore.ieee.org
... Since the **concatenation** of these two fields ... usual criterion for a **hash** function is ... Algorithms for **key generation**, authentication and confidentiality - within ...
Cited by 4 - Related articles - Web Search - All 2 versions

How to enhance the security of public-**key** encryption at minimum cost- ▶ kfupm.edu.sa [PDF]
E Fujisaki, T Okamoto - Lecture Notes in Computer Science, 1999 - Springer
... Shoup scheme under the universal one-way **hash** assumption and ... Moreover, let || denote the **concatenation** operator and, for n ... K, the **key-generation** algorithm, is a ...
Cited by 152 - Related articles - Web Search - BL Direct - All 17 versions

[PS] ▶ Visual **hash** for oblivious watermarking
J Fridrich - PROC SPIE INT SOC OPT ENG, 2000 - ws.binghamton.edu
... we require that when approximately half of the **hash** is incorrect ... random number **generator** (PRNG) seeded with a **concatenation** of the secret **key**, the block ...
Cited by 62 - Related articles - View as HTML - Web Search - All 11 versions

Practical Approaches to Attaining Security against Adaptively Chosen Ciphertext Attacks (Extended ...- ▶ kfupm.edu.sa [PDF]
Y Zheng, J Seberry - Proceedings of the 12th Annual International Cryptology ..., 1992 - Springer
... the second on the use of univer- sal **hash** functions and the ... over C is denoted by 1x1, and the **concatenation** of two ... C, E, D). C is called a **key-generation** al- ...
Cited by 41 - Related articles - Web Search - BL Direct - All 10 versions

[BOOK] LOKI: A cryptographic primitive for authentication and secrecy applications- ▶ psu.edu [PDF]

L Brown, J Seberry, J Pieprzyk, Dept. of Computer ... - 1990 - Springer
... 1 The DBH block is formed by **concatenating** the final ... the addition modulo 2 of the previous **hash** value to ... current message block before using it as **key** input to ...
Cited by 101 - Related articles - Web Search - Library Search - All 20 versions

Method and apparatus for verifiably providing **key** recovery information in a cryptographic system
R Gennaro, PA Karger, SM Matyas Jr, M Peyravian, ... - US Patent 5,907,618, 1999 - Google Patents
... The parties may derive a symmetric encryption **key** ... as **concatenating** it with another value and **hashing** the ... **concatenation** result, as described in the copending ...
Cited by 5 - Related articles - Web Search - All 2 versions

Pseudorandom number generator with backup and restoration capability
RS DeBellis, RM Smith Sr, PCC Yeh - US Patent 6,104,810, 2000 - Google Patents
... a secret value and passing the **concat**- enation result ... **hash** function to generate a **hash** value from ... functions (not shown) for encryption, **key** management, digital ...
Cited by 4 - Related articles - Web Search - All 2 versions

Robust **hash** functions for digital watermarking- ▶ binghamton.edu [PDF]
J Fridrich, M Goljan - Information Technology: Coding and Computing, 2000. ..., 2000 - ieeexplore.ieee.org
... we require that when approximately half of the **hash** is incorrect ... random number **generator** (PRNG) seeded with a **concatenation** of the secret **key**, the block ...
Cited by 93 - Related articles - Web Search - All 10 versions

On password-based authenticated **key** exchange using collisionful **hash** functions- ▶ kfupm.edu.sa [PDF]
S Bakhtiari, R Safavi-Naini, J Pieprzyk - Information Security and Privacy: First Australian ..., 1996 - books.google.com
... to as the AL protocol) where the basic Diffie-Hellman **key** exchange is ... 30 1 where ft () is a collision-free **hash** function and'||'denotes **concatenation**. ...
Cited by 11 - Related articles - Web Search - BL Direct - All 6 versions

[PDF] ▶ Secure **Key** Recovery
R Gennaro, P Karger, S Matyas, M Peyravian, A ... - IBM Thomas J. Watson Research Center, 1999 - securitytechnet.com
... R from the resultant encrypted K, as in: fKKa1.1(fKKa2.1(K)) - R. For example, if the session **key** K is ... where **Hash**() is the **hash** of the **concatenation** of the ...
Cited by 4 - Related articles - View as HTML - Web Search - All 11 versions

Secure deterministic encryption **key** generator system and method
GL Fielder, PN Alito - US Patent 5,963,646, 1999 - Google Patents
... 17, 1995 Secure **hash** algorithms were originally used 65 ... surprising, therefore, that the merely **concatenated** before being ... does not employ an A-**Key** of sufficient ...
Cited by 4 - Related articles - Web Search - All 6 versions

File encryption method and system
GL Fielder, PN Alito - US Patent 6,049,612, 2000 - Google Patents
... of the **key generator** operation and **concatenate** each pass ... previous pass(es) to create a **key** length greater ... digest length normally created by the **hash** function. ...
Cited by 2 - Related articles - Web Search - All 4 versions

Probabilistic signature scheme
M Bellare, P Rogaway - US Patent App. 09/879,849, 2001 - Google Patents
... message M, for example, by **concatenating** these strings and applying some crypto-graphic **hash** function (such ... the definition of the **key generation** and signing ...

Cited by 3 - Related articles - Web Search - All 4 versions

Public **key** cryptosystem **key** management based on control vectors

SM Matyas, DB Johnson, AV Le, R Prymak, WC Martin, ... - US Patent 5,200,999, 1993 - Google Patents

... RECORD WITH PUO TO PRODUCE ePUO (**KEY** RECORD) 521 **CONCATENATE** CONTROL VECTOR AND **KEY** RECORD TO **...** IN 522 CALCULATE HASH2 ON HA-IN WITH **HASH** ALGORITHM ha2 **...**

Cited by 23 - Related articles - Web Search - All 5 versions

ESIGN: An efficient digital signature implementation for smart cards

A Fujioka, T Okamoto, S Miyaguchi - Advances in Cryptology--EUROCRYPT'91 (LNCS 547), 1991 - Springer

... X, and \Xle4 denotes the byte size of X. allb denotes the **concatenation** of a **...** The secret **key ...** where H is a one-way **hash** function (H (M) E ZN for any positive **...**

Cited by 40 - Related articles - Web Search

[PDF] LFSR-based hashing and authentication

H Krawczyk - Lecture Notes in Computer Science, 1994 - dsns.csie.nctu.edu.tw

... for applications (as suggested here) where the **key** is changed **...** and Smeets, B., "On Families of **Hash** Functions via Geometric Codes and **Concatenation**", Proc. **...**

Cited by 159 - Related articles - Web Search - All 2 versions

Fast message authentication using efficient polynomial evaluation

V Afanassiev, C Gehrmann, B Smeets - Lecture notes in computer science, 1997 - Springer

... The construction is a **concatenation** of a 1/2 r - AU 2 family of **hash** functions **...** IF Q and x,y ∈ IF Q , z ∈ IF q as the **key** parts gives us the corresponding **...**

Cited by 15 - Related articles - Web Search - BL Direct - All 5 versions

[PDF] TSH-ESIGN: Efficient Digital Signature Scheme Using Trisection Size **Hash** (Submission to P1363a)

T Okamoto, E Fujisaki, H Morita - 1998 - crypto.nknu.edu.tw

... H(x) can be realized by using **hash** function H : {0;1 **...** Moreover, || denotes the **concatenation ... Key generation** algorithm **Gen** is a probabilistic polynomial-time **...**

Cited by 3 - Related articles - View as HTML - Web Search - All 5 versions

Fully-fledged two-way public **key** authentication and **key** agreement for low-cost terminals

MJ Beller, Y Yacobi, RB Bellcore - Electronics Letters, 1993 - ieeexplore.ieee.org

... Rabin secret **key** (p, q,), and gives the corresponding public **key** (N, p **...** using the modular square root oper- ation to sign a **hashing** of the **concatenation** of j **...**

Cited by 71 - Related articles - Web Search - BL Direct - All 3 versions

User impersonation in **key** certification schemes

AK Lenstra, Y Yacobi - Journal of Cryptology, 1993 - Springer

... User Impersonation in **Key** Certification Schemes **...** function of 14 and NA: it might simply **concatenate** 14 and **...** in any order, interleave their bits, or **hash** them in **...**

Cited by 4 - Related articles - Web Search - BL Direct - All 3 versions

[PDF] Internet security architecture

R Molva - Computer Networks-the International Journal of Computer and ..., 1999 - Citeseer

... that is based on the secure **hash** function H **...** TLS Handshake Protocol, - | denotes the **concatenation** - s is a **...** security function from the master **key** established by **...**

Cited by 39 - Related articles - View as HTML - Web Search - All 8 versions

[PDF] The secure remote password protocol

T Wu... - Proceedings of the 1998 Internet Society Network and ..., 1998 - eprints.kfupm.edu.sa

... P The user's password x A private **key** derived from **...** A;B Corresponding public keys

H One-way **hash** function m **...** two quantities strings m and n **concatenated** K Session **...**
Cited by 364 - Related articles - View as HTML - Web Search - All 74 versions

[CITATION] Temporal **key hash**
R Housley, D Whiting - IEEE P802. 11 Wireless LANs, 2001
Cited by 12 - Related articles - Web Search

Method and apparatus for protecting the confidentiality of passwords in a distributed data ...
CW Kaufman, M Gasser, BW Lampson, JJ Tardo, K ... - US Patent 5,497,421, 1996 - Google Patents
... gener- ates a random bit string to which is **concatenated** a **hash**- coded version of **...**
is 35 encrypted under the authentication server's public **key** and forwarded **...**
Cited by 41 - Related articles - Web Search - All 4 versions

Signing with partially adversarial hashing
S Micali, L Reyzin - 1998 - portal.acm.org
... executing the scheme, one needs to pick a **hash** function **...** private **key** and (n; 3) as
the public **key**. **...** jjG 2 (w) (here \ jj " denotes **concatenation** of strings **...**
Cited by 1 - Related articles - Web Search - All 7 versions

Secure Transport of Authentication Data in Third **Generation** Mobile Phone Networks
S Pütz, R Schmitz, B Tietz - Lecture notes in computer science, 1999 - Springer
... of applying a collision-resistant one-way **hash**- function to **...** network X KS XY (i)
Symmetric session **key** #i for **...** data from X to Y m1||m2 **Concatenation** of message **...**
Cited by 1 - Related articles - Web Search - BL Direct - All 4 versions

[PS] ⮞MIME object security services: Issues in a multi-user environment
JM Galvin, MS Feldman - Proceedings of the 5th conference on USENIX UNIX Security ..., 1995 - se.kde.org
... eg, a favorite quotation or other **concatenation** of many **...** MOSS uses the MD5 [13] **hash**
algorithm for **...** Unpredictable bits are required for **key generation** and for **...**
Cited by 3 - Related articles - View as HTML - Web Search - All 18 versions

A compact and fast hybrid signature scheme for multicast packet authentication
P Rohatgi - Proceedings of the 6th ACM conference on Computer and ..., 1999 - portal.acm.org
... include a commitment, in a theoretical setting the public **key** can be **...** where "|" denotes
concatenation. **...** as both a commitment to T and a collision resistant **hash**. **...**
Cited by 126 - Related articles - Web Search - All 5 versions

[PDF] ⮞Optimistic fair exchange of digital signatures
N Asokan, V Shoup, M Waidner - IEEE Journal on Selected Areas in Communications, 2000 - Citeseer
... Key generation for DSS is identical to that for the Schnorr scheme **...** computes r =
(g k) mod q and s = k ?1 (H(m)+xr), where H is a **hash** function with outputs in **...**
Cited by 429 - Related articles - View as HTML - Web Search - Library Search - BL Direct - All 14 versions

High-speed implementation of an ECC-based wireless authenticationprotocol on an ARM microprocessor- ⮞oregonstate.edu [PDF]
M Aydos, T Yanik, CK Koc - IEE Proceedings-Communications, 2001 - ieeexplore.ieee.org
... field GF(29, and provides fast public-**key** operations **...** operations, the digital signature
generation and verification, and the secure **hash** algorithm SHA **...**
Cited by 55 - Related articles - Web Search - BL Direct - All 24 versions

Kleptography: Using cryptography against cryptography
A Young, M Yung - Lecture Notes in Computer Science, 1997 - Springer
... Let p is a large strong prime and g is a **generator** mod p. The **...** public **key** be Y . Let
W be a fixed odd integer, and let H be a **...** strong **hash** function. **...**

Cited by 54 - Related articles - Web Search - Library Search - BL Direct - All 8 versions

CRC **hash** compressed server object identifier

PF Rieth, JS Stevens - US Patent 6,134,597, 2000 - Google Patents

... by CRC **hashing** a string formed by **concatenating** a user **...** object is authorized only upon CRC **hashing** to the **...** Sheets 42 PROFILE USER ID HIDDEN **KEY** COMPRESSED CRC **...**

Cited by 4 - Related articles - Web Search - All 2 versions

On the existence of statistically hiding bit commitment schemes and fail-stop signatures

IB Damgård, TP Pedersen, B Pfitzmann - Journal of Cryptology, 1997 - Springer

... commitments plus universal and collision-intractable **hash** functions. **...** all signatures made with that **key**: In the **...** a security parameter k. The **concatenation** of all **...**

Cited by 74 - Related articles - Web Search - BL Direct - All 8 versions

Practical invisibility in digital communication- ⏩psu.edu [PDF]

T Aura - Lecture Notes in Computer Science, 1996 - Springer

... A pseudorandom fimetion **generator** is easily constructed from any secure **hash** fimction H, such as SHS, by **concatenating** the argument i with a secret **key** K and **...**

Cited by 35 - Related articles - Web Search - BL Direct - All 12 versions

Non-repudiation without public-**key**

R Taylor - Lecture Notes in Computer Science, 1996 - Springer

... B. Smeets, On families of **Hash** functions via Geometric Codes and **Concatenation**, Advances in **...** An Optimal class of Symmetric **Key Generation** Systems, Advances **...**

Cited by 4 - Related articles - Web Search - BL Direct - All 3 versions

Cryptographic **key generation** using sequential **concatenation**.

D Coppersmith, PW Rogaway, P It - 1995 - freepatentsonline.com

... values as mixed in step (c); (e) **concatenating** into the **...** 1 or claim 2 wherein the **key** is preprocessed **...** pseudorandom **generator** derived from a secure **hash** algorithm **...**

Related articles - Web Search - All 3 versions

Method for encryption **key generation**

JW Weber, JW Fahrny - US Patent App. 10/035,636, 2001 - Google Patents

... is reduced by means of the secure **hash** algorithm. **...** the encryption **key** is a **concatenation** of all **...** to the present method for encryption **key generation** prevents a **...**

Web Search - All 2 versions

[PDF] ⏩Arbitration in Tamper Proof Systems

GIDBJ Matt - Advances in Cryptology--CRYPTO'87: Proceedings, 1988 - tcs.ics.saitama-u.ac.jp

... user B user A's secret **key** and the public **key** of user **...** message counter mc and time stamp is are **concatenated** to the message and a cryptographic **hash** ch is **...**

Related articles - Web Search - All 2 versions

Key recovery condition encryption and decryption apparatuses

H Miyauchi, K Sako, M Yamazaki, S Domyo, H ... - US Patent 6,272,225, 2001 - Google Patents

... the **hash** value from said **hashing** device to **...** condition information encryptor that encrypts a **concat**- enating result **...** concatenator by using a random **key** from said **...**

Related articles - Web Search - All 5 versions

Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number

J Kelsey, B Schneier, N Ferguson - Selected Areas in Cryptography: 6th Annual International ..., 2000 - books.google.com

... for the **generator** from the entropy accumulator's pool and the existing **key**. ... steps:
1. The entropy accumulator computes the **hash** on the **concatenation** of all ...
Related articles - Web Search

Methods and systems for defeating TCP SYN flooding attacks
M Lamberton, E Levy-Abegnoli, P Thubert - US Patent App. 09/755,564, 2001 - Google Patents
... 620K [614 {616] Get Current **Key** [618] Pick Up a Category **CONCATENATE**: {Current **Key**, Client Socket, Server Socket} [630^ I **HASH**: {Current **Key** ...
Related articles - Web Search - All 5 versions

Fast and secure hashing based on codes- ⏩ kuleuven.be [PDF]
L Knudsen, B Preneel - Lecture Notes in Computer Science, 1997 - Springer
... cipher with **key** Ii: The variables Hlo and H20 are initialized with the values IV1 and IVz respec- tively, and the **hash** result is equal to the **concatenation** of ...
Cited by 30 - Related articles - Web Search - BL Direct - All 10 versions

[BOOK] Improving resistance to differential cryptanalysis and the redesign of LOKI
L Brown, Dept. of Computer Science, ADF Academy, ... - 1991 - Springer
... detailed its application to FEAL and N-**Hash** [4], and ... Since 28/4096 2 -r' if we **concatenate** these characteristics ... discovered a weakness in the LOKI89 **key** schedule ...
Cited by 70 - Related articles - Web Search - Library Search - BL Direct - All 11 versions

Secret communication and authentication scheme based on public **key** cryptosystem using N-adic ...
T Takagi, S Naito... - US Patent 6,259,790, 2001 - Google Patents
... PROCESSING UNIT U AUTHENTICATION MESSAGE **HASHING** PROCESSING UNIT en DATA COUPLING PROCESSING UNIT **KEY** GENE PROCESSI ... DH U co DATA **CONCATENATION** PROCESSING UNIT ...
Related articles - Web Search - All 4 versions

Cryptographic facility environment backup/restore and replication in a public **key** cryptosystem
SM Matyas, DB Johnson, AV Le, R Prymak, WC Martin, ... - US Patent 5,265,164, 1993 - Google Patents
... PC Pi)RTABLE \RT 104'^ LDIDa US LDIDb US' Y F/G.9 PORTABLE PART 104 SECRET PART 150^ MASTER **KEY** REGISTER(S) 151 PSEUDORANDOM NUMBER **GENERATOR** SEED **KEY**(S) 152 ...
Cited by 35 - Related articles - Web Search - All 4 versions

Method and apparatus for improved pseudo-random number **generation**
MJ Saarinen - US Patent App. 09/859,274, 2001 - Google Patents
... These two **hash** functions each operate on the **concatenation** of a chosen constant value in base 16, the current internal **key** K, the current seed value S ...
Cited by 1 - Related articles - Web Search - All 6 versions

Hash table implementation of an object repository
RG Hunt - US Patent 6,154,747, 2000 - Google Patents
... implements the inventive method includes a first **hash** table for storage of data representing the object with an object identifier used as a **key** for storage of ...
Cited by 4 - Related articles - Web Search - All 2 versions

[PDF] ⏩ Cryptanalysis and improvement of Petersen-Michels signcryption scheme
WH He, TC Wu - IEE Proceedings-Computers and Digital Techniques, 1999 - ntur.lib.ntu.edu.tw
... **key**, U, first computes the encryp- tion **key** as K=zllf(m, z), where '11' is the **concatenation** operator, and ... m, z) is equivalent to the **hash** value of the ...
Cited by 23 - Related articles - View as HTML - Web Search - BL Direct - All 5 versions

[PDF] ⏩ pStore: A secure peer-to-peer backup system

C Batten, K Barr, A Saraf, S Trepetin - Unpublished report, MIT Laboratory for Computer Science, 2001 - eprints.kfupm.edu.sa
... filename identifier is formed by first **concatenating** the private **...** 17], and SHA-1 for cryptographic **hashing** [16]. **...** as well as pub- lic and private **key generation**. **...**
Cited by 62 - Related articles - View as HTML - Web Search - All 25 versions

Efficient and generalized group signatures- ▶uwaterloo.ca [PDF]
J Camenisch - Lecture Notes in Computer Science, 1997 - Springer
... and let g E G be a **generator** of G such that computing **...** computing yi = gx* with the secret **key** zi chosen at random from Z **...** (1 denotes the **concatenation** of two **...**
Cited by 209 - Related articles - Web Search - BL Direct - All 5 versions

Distributed authentication system and method
TR Spies, PK Misra - US Patent 6,230,269, 2001 - Google Patents
... As an example, this session **key** can be constructed for use in a **...** client 26 constructs a message M to contain a **concatenated** string of the first **hash** value H **...**
Cited by 7 - Related articles - Web Search - All 2 versions

Pseudorandom number generator with normal and test modes of operation
RS DeBellis, RM Smith Sr, PCC Yeh - US Patent 6,061,703, 2000 - Google Patents
... a secret value and passing the **concat**- enation result **...** **hash** function to generate a **hash** value from **...** functions (not shown) for encryption, **key** management, digital **...**
Cited by 2 - Related articles - Web Search - All 2 versions

From fixed-length to arbitrary-length RSA padding schemes- ▶psu.edu [PDF]
JS Coron, F Koeune, D Naccache - Lecture notes in computer science, 2000 - Springer
... nor as- sume the existence of collision-resistant **hash**-functions **...** we let m 1 ||m 2 denote the **concatenation** of **...** 0, 1} k+1 → {0, 1} k **Key generation** : Generate {N **...**
Cited by 4 - Related articles - Web Search - BL Direct - All 20 versions

MDx-MAC and building fast MACs from **hash** functions- ▶kuleuven.be [PDF]
B Preneel, PC Van Oorschot - Lecture Notes in Computer Science, 1995 - Springer
... The secret **key** can be introduced in the IV, in the **...** collision resistance for **hash** functions). **...** the MAC for z' 11 y is the same (here 11 denotes **concatenation**). **...**
Cited by 135 - Related articles - Web Search - BL Direct - All 40 versions

Method, system and apparatus for generating self-validating prime numbers
SM Matyas Jr, A Roginsky - US Patent 6,307,938, 2001 - Google Patents
... 120 bits are taken from the resulting **hash** value **...** The **concatenation** of the 7 SEED values used in generating **...** X^SEED) be retained with the private **key** as evidence **...**
Cited by 5 - Related articles - Web Search - All 2 versions

MMH: Software message authentication in the Gbit/second rates
S Halevi, H Krawczyk - Lecture notes in computer science, 1997 - Springer
... the function h and the seed s to the pseudo-random **generator** (s can also be a **key** to a **...** function to the output of the **hash** function **concatenated** with a **...**
Cited by 84 - Related articles - Web Search - BL Direct - All 11 versions

Authentication and authenticated **key** exchanges- ▶psu.edu [PDF]
W Diffie, PC Oorschot, MJ Wiener - Designs, Codes and Cryptography, 1992 - Springer
... {x, y } is the result when a **hash** function is applied to x **concatenated** with y. Alice's secret **key** for a signature scheme, sA(x) is Alice's signature on x. **...**
Cited by 692 - Related articles - Web Search - All 12 versions

Method for human-assisted random **key generation** and application for digital watermark system
SA Moskowitz, M Cooperman - US Patent 5,822,432, 1998 - Google Patents
... Chapter 12.1: Public-**Key** Algo- rithms Background, pp **...** 273-275, Chapter 14.1: One-Way **Hash** Functions, Background **...** for the human-assisted **generation** and application **...**
Cited by 23 - Related articles - Web Search - All 2 versions

[PDF] Secure conference **key** distribution schemes for conspiracy attacks
K Koyama - Lecture Notes in Computer Science, 1993 - hacktic.nl
... the exponents Xj and Alj4 respectively, where || denotes **concatenation**. **...** with a public one-way **hash** function h **...** user 1 in the subsequent **key generation** procedure **...**
Cited by 20 - Related articles - Web Search - BL Direct - All 2 versions

Security of authenticated multiple-**key** agreement protocols
TS Wu, WH He, CL Hsu - Electronics Letters, 1999 - ieeexplore.ieee.org
... turbo codes: Some results on parallel **concatenated** coding schemes **...** it holds, B proceeds to the **key generation** phase and **...** simply employ a one-way **hash** function h **...**
Cited by 16 - Related articles - Web Search - BL Direct - All 3 versions

One-way functions are necessary and sufficient for secure signatures- princeton.edu [PDF]
J Rompel - Proceedings of the twenty-second annual ACM symposium on ..., 1990 - portal.acm.org
... key PK, we would be able to ob- tain a secret **key** SW with **...** We will denote the **concatenation** of strings x and y by x • y. We will **...** 3 Constructing a One-way **Hash ...**
Cited by 350 - Related articles - Web Search - All 4 versions

Fortifying **key** negotiation schemes with poorly chosen passwords
RJ Anderson, TMA Lomas - Electronics letters, 1994 - ieeexplore.ieee.org
... cols which use passwords to augment Diffie Hellman **key** exchange, most **...** h is a suitable one-way collision-free **hash** function and I denotes **concatenation**. **...**
Cited by 39 - Related articles - Web Search - BL Direct - All 3 versions

Key Management Techniques
W Fumy - Lecture notes in computer science, 1998 - Springer
... An example for a **key** calculation function is applying a cryptographic **hash**-function to the **concatenation** of the data items, eg, K = **hash**(K AB || X **...**
Cited by 3 - Related articles - Web Search - BL Direct - All 4 versions

Key authors: **H Krawczyk** - **M Bellare** - **N Haller** - **S Fluhrer** - **R Canetti**

Gooooooooogle
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

hash concatenation key generation Search

Scholar **All articles** - Recent articles Results **1** - **100** of about **271** for **hash concatenate key video**

Did you mean: ***bash*** concatenate key video distribution

Scrambling and **key distribution** scheme for digital television
W Kanjanarin, T Amornraksa - Ninth IEEE International Conference on Networks, 2001. ..., 2001 - ieeexplore.ieee.org
... and a **hash** value calculated from a strong collision resistant one-way **hash** function (h **...** i = 2,3,.n/2 6. Set ML' as the **concatenation** of ML **...** **Key distribution** scheme **...**
Cited by 12 - Related articles - Web Search - All 3 versions

Robust **hash** functions for digital watermarking- binghamton.edu [DOC]
J Fridrich, M Goljan - Information Technology: Coding and Computing, 2000. ..., 2000 - ieeexplore.ieee.org
... we require that when approximately half of the **hash** is incorrect **...** random number generator (PRNG) seeded with a **concatenation** of the secret **key**, the block **...**
Cited by 93 - Related articles - Web Search - All 10 versions

[PS] Visual **hash** for oblivious watermarking
J Fridrich - PROC SPIE INT SOC OPT ENG, 2000 - ws.binghamton.edu
... we require that when approximately half of the **hash** is incorrect **...** random number generator (PRNG) seeded with a **concatenation** of the secret **key**, the block **...**
Cited by 62 - Related articles - View as HTML - Web Search - All 11 versions

ELK, a new protocol for efficient large-group **key distribution**- cmu.edu [PDF]
A Perrig, D Song, D Tygar - 2001 IEEE Symposium on Security and Privacy, 2001. S&P 2001. ..., 2001 - ieeexplore.ieee.org
... are interested in situations where we have widespread **video** or au **...** To encrypt message M with **key** K we write {M}K **...** To **concatenate** the messages MI and M2 we write MI **...**
Cited by 237 - Related articles - Web Search - BL Direct - All 21 versions

Robust bit extraction from images- binghamton.edu [PS]
J Fridrich - IEEE International Conference on Multimedia Computing and ..., 1999 - ieeexplore.ieee.org
... Such techniques are not truly oblivious because the **hash** needs to **...** random number generator (PRNG) seeded with a **concatenation** of the secret **key**, the block **...**
Cited by 49 - Related articles - Web Search - All 12 versions

System and method for secure font subset **distribution**
DR Simon, J Benaloh, DD Chinn, G Hitchcock, D ... - US Patent 6,065,008, 2000 - Google Patents
... The authentication module also produces an unsigned root by using the public **key** of the font **...** This root is formed from **concatenating** the **hash** values of all **...**
Cited by 10 - Related articles - Web Search - All 2 versions

System and method for ensuring integrity of audio
DL Davis - US Patent 5,946,396, 1999 - Google Patents
... with an entity, encrypted by a private **key** held by **...** digests 310 and 315 may be **concat** -enated and **...** Normally, the **hash** algorithms are the same, although different **...**
Cited by 3 - Related articles - Web Search - All 2 versions

Method for encryption **key** generation
JW Weber, JW Fahrny - US Patent App. 10/035,636, 2001 - Google Patents
... is reduced by means of the secure **hash** algorithm **...** previously discussed, the encryption **key** is a **concatenation** of all **...** of a use for an encryption **key** that expires **...**
Web Search - All 2 versions

[PDF] ▶ Fragile watermarking using the VW2D watermark
RB Wolfgang, EJ Delp - Proc. SPIE, Security and Watermarking of Multimedia Contents, 1999 - cerias.purdue.edu
... of the previous request time, request and the **hash** of the **...** C n . The TSS signs this **concatenation**, which forms the **...** K PRI is the private **key** of the TSS and F is **...**
Cited by 96 - Related articles - View as HTML - Web Search - All 11 versions

A prepositioned secret sharing scheme for message authentication in broadcast networks- ▶ cuny.edu [PDF]
AM Eskicioglu - Proceedings of the Communications and Multimedia Security …, 2001 - books.google.com
... of message M with an MDC; h^ M): **Hashing** of message **...** a MAC with **key** K; M,|| M2: **Concatenation** of message **...** also be used to build a convenient **key** transport scheme **...**
Cited by 6 - Related articles - Web Search - All 7 versions

Overview of image security techniques with applications in multimedia systems- ▶ kfupm.edu.sa [PDF]
RB Wolfgang, EJ Delp - Proceedings of the SPIE International Conference on …, 1997 - eprints.kfupm.edu.sa
... request time, identification string, document **hash** and linking string **hash**. **...** next request, I n+1 , then **concatenates** it to **...** where K PRI is the private **key** of the **...**
Cited by 49 - Related articles - View as HTML - Web Search - All 14 versions

A perceptual audio hashing algorithm: a tool for robust audio identification and information hiding- ▶ boun.edu.tr [PDF]
MK Mihcak, R Venkatesan - Inf. Hiding, 2001 - Springer
... the stream (eg each frame of a **video** sequence) after **...** The secret **key** K is used as the seed of **...** the reconstruction levels are not crucial for **hashing** problem as **...**
Cited by 44 - Related articles - Web Search - BL Direct - All 11 versions

Hierachical brushing in a collection of **video** data- ▶ mac.com [PDF]
D Ponceleon, A Dieberger - PROCEEDINGS OF THE ANNUAL HAWAII INTERNATIONAL CONFERENCE ON …, 2001 - csdl.computer.org
... Region **Hashing** is a technique used to discover the **...** It is generated by **concatenating** strips (typically from **...** Komlodi, A., and Marchionini, G., **Key** frame preview **...**
Cited by 29 - Related articles - Web Search - BL Direct - All 8 versions

Cryptographic **key** generation using sequential concatenation.
D Coppersmith, PW Rogaway, P It - 1995 - freepatentsonline.com
... A and B. The symbol "| |" denotes the **concatenation** operator **...** National Institute of Standards, "Secure **Hash** Standard," Federal **...** In particular, **key** a is mapped by A **...**
Related articles - Web Search - All 3 versions

Similarity search in high dimensions via hashing- ▶ kfupm.edu.sa [PDF]
A Gionis, P Indyk, R Motwani - In Proc. 25th Internat. Conf. on Very Large Data Bases, 1999 - eprints.kfupm.edu.sa
... The **key** idea is to **hash** the pointsusingseveralhashfunctionssoastoensure that **...** positions as per I and **concatenating** the bits **...** we use two levels of **hash**- ing: the **...**
Cited by 434 - Related articles - View as HTML - Web Search - BL Direct - All 7 versions

[PDF] ELK, a New Protocol for Efficient Large-Group **Key Distribution**
APDSJD Tygar - Proc. of IEEE Security and Privacy Symposium S&P2001, 2001 - cs.berkeley.edu
... We are interested in situations where we have widespread **video** or au- dio streaming over a **...** To encrypt message with **key** ¡ we write **...** To **concatenate** the messages **...**
Related articles - View as HTML - Web Search - All 4 versions

[PDF] Feature-based **Video** Sequence Identification
KM Pua - 1995 - Citeseer
... video archive size……95 6.2 Graph of **video** sequence **hashing** time versus **...** Instead of selecting still images as **key**-frames for **video** sequences, Arman [3 **...**
View as HTML - Web Search - All 8 versions

Method for human-assisted random **key** generation and application for digital watermark system
SA Moskowitz, M Cooperman - US Patent 5,822,432, 1998 - Google Patents
... 273-275, Chapter 14.1: One-Way **Hash** Functions, Background **...** METHOD FOR HUMAN-ASSISTED RANDOM **KEY** GENERATION AND **...** such as musical recordings, movies, and **video** games **...**
Cited by 23 - Related articles - Web Search - All 2 versions

Addressing weaknesses in two cryptographic protocols of Bull, Gongand Sollins
AM Mathuria - Electronics Letters, 1995 - ieeexplore.ieee.org
... one-way **hash** function, where k is a **key** and m is **...** sense of a secure keyed one-way **hash** function (SKOWHF **...** and m and n denotes the bitwise **concatenation** of messages **...**
Cited by 3 - Related articles - Web Search - BL Direct - All 3 versions

MARKS: Zero side effect multicast **key** management using arbitrarily revealed **key** sequences- ucl.ac.uk [PDF]
B Briscoe - Lecture Notes in Computer Science, 1999 - Springer
... Note that one MD5 **hash** (portable source) of a 128b input **...** between security and the convenience of a continuous **key**-space (as against **concatenating** BHTs side **...**
Cited by 108 - Related articles - Web Search - BL Direct - All 15 versions

Adaptive block matching motion estimation algorithm for videocoding
J Feng, KT Lo, H Mehrpour, AE Karbowiak - Electronics letters, 1995 - ieeexplore.ieee.org
... one-way **hash** function, where k is a **key** and m is **...** sense of a secure keyed one-way **hash** function (SKOWHF **...** and m and n denotes the bitwise **concatenation** of messages **...**
Cited by 25 - Related articles - Web Search - BL Direct - All 3 versions

Software anti-piracy system that adapts to hardware upgrades
DB Pearce, A Hughes - US Patent 6,243,468, 2001 - Google Patents
... Once the purchaser enters the same **key** more times than a defined limit, the product is disabled. **...** One preferred approach is to **hash** the **concatenation** of the **...**
Cited by 7 - Related articles - Web Search - All 2 versions

Content packet **distribution** system
RW Schumann, R Whittemore, DM Goldschlag, DW … - US Patent App. 09/880,855, 2001 - Google Patents
... computer negotiate access and a **key** changes each **...** depicting exemplary audio and **video** streams laid **...** an exemplary digital content **distribution** system according to **...**
Web Search - All 4 versions

Software performance of universal **hash** functions- saitama-u.ac.jp [PDF]
W Nevelsteen, B Preneel - Lecture notes in computer science, 1999 - Springer
... bucket **hashing**, bucket **hashing** with a short **key**, fast polynomial **...** of the buckets is computed, and the **hash** function output is the **concatenation** of the **...**

Cited by 37 - Related articles - Web Search - BL Direct - All 15 versions

Method and apparatus for providing conditional access in connection-oriented interactive networks ...
AH Wasilewski, DF Woodhead, GL Logston - US Patent App. 09/135,615, 1998 - Google Patents
... for ensuring that programs comprising at least one of **video**, audio, and ... 2002/0094084 Al CLEAR EMM 1020 ONE-WAY **HASH** FUNCTION (eg, MD5) PUBLIC-**KEY** ENCRYPT (eg ...
Cited by 31 - Related articles - Web Search - All 7 versions

[PDF] An extendible **hash** for multi-precision similarity querying of image databases
S Lin, MT Ozsu, V Oria, R Ng - PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON VERY LARGE ..., 2001 - Citeseer
... but fails for non-uniform data **distribution** because of ... ous to the original one, ¤ ¢ ¦ (since the **key** space doubles ... Therefore two keys that **hash** to the same ...
Cited by 27 - Related articles - View as HTML - Web Search - BL Direct - All 15 versions

Flow identification for supporting per-flow queueing
Z Cao, Z Wang - Computer Communications and Networks, 2000. Proceedings. ..., 2000 - ieeexplore.ieee.org
... a data item distinguished by its "**key**" into one of a ... of Five-Tuple This **hash** function **concatenates** all bits ... the performance of the perfect **hash** function we ...
Cited by 3 - Related articles - Web Search

Apparatus and method for encryption **key** generation
T Butler, M Wong - US Patent 6,094,487, 2000 - Google Patents
... Use of a **hashing** algorithm to convert at ... other SSD field by simply **concatenating** additional infor ... example, this method for encryption **key distribution** can be ...
Cited by 2 - Related articles - Web Search - All 2 versions

Time-bracketing infrastructure implementation
DL Davis - US Patent 5,966,446, 1999 - Google Patents
... according to any bit manipulation including addition, **concatenation**, concurrent **hashing**, and the ... A "**key**" is an encoding and/or decoding parameter ...
Cited by 4 - Related articles - Web Search - All 2 versions

Practical invisibility in digital communication- psu.edu [PDF]
T Aura - Lecture Notes in Computer Science, 1996 - Springer
... fimetion generator is easily constructed from any secure **hash** fimction H, such as SHS, by **concatenating** the argument i with a secret **key** K and ...
Cited by 35 - Related articles - Web Search - BL Direct - All 12 versions

Secure electronic content **distribution** on CDS and DVDs
MM Hurtado, KL Milsted, GG Gruse, E Downs, CT ... - US Patent App. 09/376,102, 1999 - Google Patents
... 5,2003 (54) SECURE ELECTRONIC CONTENT **DISTRIBUTION** ON CDS AND DVDS (76 ... end user system receives a secure container containing the decrypting **key** for decrypting ...
Cited by 4 - Related articles - Web Search - All 5 versions

An evaluation of the **key** design criteria to achieve high updaterates in packet classifiers
C Macian, R Finthammer - IEEE Network, 2001 - ieeexplore.ieee.org
... is that for any packet P, the **concatenation** C of ... current proposals led us to identify three **key** parameters that ... filter is included in the respective **hash** table ...
Cited by 20 - Related articles - Web Search - BL Direct - All 4 versions

Programming content **distribution**
JT Hurst, RJ Fuoco, WE Elswick - US Patent App. 09/784,843, 2001 - Google Patents

... file can be done easily, by **concatenating** the contents ... asset encryp- tion and encryption **key** management preferably ... in three languages and two **video** formats, a ...
Web Search - All 2 versions

0 IEE 1998 Electronics Letters Online No: 19980714
SH Kim, HG Kim - Trans. Circuits Syst. **Video** Technol, 1997 - ieeexplore.ieee.org
... However, if a **hash**- function such as SHA-1 is used ... the encryption of data X using the secret **key** KAB (shared by A and B), TIY denotes the **concatenation** of data ...
Web Search

Content protection for digital transmission systems
CBS Traw, DW Aucsmith - US Patent App. 08/909,338, 1997 - Google Patents
... DSS with public **key** X1 [0054] E[K, M]=Encrypt M with **key** K using baseline cipher [0055] HSHA.1[M]=Add SHA-1 **hash** to M [0056] ^**Concatenation** of fields ...
Cited by 1 - Related articles - Web Search - All 4 versions

Multiresolution scene-based **video** watermarking using perceptualmodels- ▶psu.edu [PDF]
MD Swanson, B Zhu, AH Tewfik - IEEE Journal on Selected Areas in Communications, 1998 - ieeexplore.ieee.org
... partially generated from the signal dependent **key**) depends on the ... to invert the one-way **hash** function, the ... coefficient frame is the block **concatenation** of all ...
Cited by 274 - Related articles - Web Search - BL Direct - All 10 versions

CRYPTOGRAPHIC DEVICE AND METHOD FOR ASSURING INTEGRITY OF TRUSTED AGENT COMMUNICATIONS
D DAVIS, H HERBERT, P It - 2000 - freepatentsonline.com
... Upon receipt, the **key** pair is stored in ... Of course, as alternative embodiments, the **hash** operation may ... with an "assertion", eg by **concatenation**, modulo addition ...
Web Search - All 5 versions

[PDF] ▶A Network Design Architecture for **Distribution** of Generic Scene Graphs
P Fiambolis, G Prolopakis, NAVAL POSTGRADUATE ... - 1999 - Citeseer
... The scope of this thesis is the design and implementation of a network architecture for **distribution** of ... Audio < 30 ms No Yes Yes **Video** < 100 ms No Yes Yes
Related articles - View as HTML - Web Search - Library Search - All 10 versions

Digital signets: Self-enforcing protection of digital information (preliminary version)- ▶kfupm.edu.sa [PDF]
C Dwork, J Lotspiech, M Naor - Proceedings of the twenty-eighth annual ACM symposium on ..., 1996 - portal.acm.org
... letting '[o" denote **concatenation**, it seems plausible that the ... example, several programs, or several images, or **video** ... a program to extricate the **key** K from ...
Cited by 84 - Related articles - Web Search - BL Direct - All 7 versions

Content-based query processing for **video** databases- ▶hinet.net [PDF]
TCT Kuo, ALP Chen - IEEE Transactions on Multimedia, 2000 - ieeexplore.ieee.org
... correlation of content objects in the **key** frames was ... positions of the content objects in **video** frames ... content objects can be represented by **concatenating** type 2 ...
Cited by 31 - Related articles - Web Search - BL Direct - All 7 versions

System for encryption of partitioned data blocks utilizing public **key** methods and random numbers
N Brandman - US Patent 5,974,144, 1999 - Google Patents
... **key** and the second secret **key**, and is **key distribution** in a ... 1 is a **video** encryption block diagram; FIG ... 2 illustrates random seed and global **key** creation; and FIG ...

Related articles - Web Search - All 2 versions

Digital watermarking by adding random, smooth patterns
J Fridrich - US Patent 6,101,602, 2000 - Google Patents
... The watermark is a **concatenation** of two or more bit ... can be obtained using classical crypto- graphic **hash** functions or ... a brute-force search for the **key** under a ...
Cited by 12 - Related articles - Web Search - All 2 versions

Natural language watermarking: Design, analysis, and a proof-of-concept implementation- ▶ purdue.edu [PS]
MJ Atallah, V Raskin, M Crogan, C Hempelmann, F ... - Lecture Notes in Computer Science, 2001 - Springer
... The secret **key** that is used to insert the watermark, and ... i) where H is a one-way **hash** function ... The watermark consists, of course, of the **concatenation** of αβ ...
Cited by 71 - Related articles - Web Search - BL Direct - All 6 versions

[PDF] ▶ Digital images protection techniques in a broadcast framework: an overview
JF Delaigle, JM Boucqueau, JJ Quisquater, B Macq - Proc. of ECMAST, 1996 - tele.ucl.ac.be
... It will be done by a **concatenation** of binary bitstreams before the H- function ... One needs the signature, the CO's public **key**, the **hash**-function and ...
Cited by 30 - Related articles - View as HTML - Web Search - All 2 versions

Platform and method for assuring integrity of trusted agent communications
DL Davis, HC Herbert - US Patent App. 09/995,994, 2001 - Google Patents
... Upon receipt, the **key** pair is stored in ... Of course, as alternative embodiments, the **hash** operation may ... with an "assertion", eg by **concatenation**, modulo addition ...
Cited by 1 - Related articles - Web Search - All 4 versions

METHOD AND APPARATUS FOR USE OF A WATERMARK AND A RECEIVER DEPENDENT REFERENCE FOR THE PURPOSE OF ...
MA EPSTEIN - US Patent App. 09/320,606, 1999 - Google Patents
... a unique receiver identifier and a private/ public **key** system is ... with the ticket (T), utilizing for instance **concatenation** and **hashing** functions, thereby ...
Web Search - All 6 versions

CBC MAC for real-time data sources- ▶ kfupm.edu.sa [PDF]
E Petrank, C Rackoff - Journal of Cryptology, 2000 - Springer
... **hash** with a second **key**, on the **concatenation** of the result to the ... breaker finds two different messages that get the same **hash** value ... **key** a 2 . Now, we may write ...
Cited by 86 - Related articles - Web Search - BL Direct - All 17 versions

Cryptography Regulations for E-commerce and Digital Rights Management.
A Torrubia, FJ Mora, L Marti - Computers & Security, 2001 - Elsevier
... the CA's digital signature, obtained by **hashing** all of ... is then encrypted using the signer's private **key**. ... for the message they receive, **concatenate** it with ...
Cited by 24 - Related articles - Web Search - All 2 versions

[BOOK] Internet QoS: architectures and mechanisms for quality of service
Z Wang - 2001 - books.google.com
... G. Messerschmitt Modern Cable Television Technology: **Video**, Voice, anil ... MPLS ARCHITECTURE 151 4.4.1 **Key** Concepts 151 4.4 ... SHARING 203 5.8.1 Direct **Hashing** 205 ...
Cited by 253 - Related articles - Web Search - Library Search - All 12 versions

Using a **hash**-based method with transaction trimming for miningassociation rules- ▶ ntu.edu.tw [PDF]

JSPMS Chen, PS Yu - IEEE Transactions on Knowledge and Data Engineering, 1997 - ieeexplore.ieee.org
... for the large 2-itemsets, is the **key** issue to ... a priori candidate generation, where * is an operation for **concatenation**. ... such counting in C 2 . A **hash** tree is ...
Cited by 298 - Related articles - Web Search - BL Direct - All 22 versions

Lower bounds for multicast message authentication- ▶ iacr.org [PDF]
D Boneh, G Durfee, M Franklin - Lecture Notes in Computer Science, 2001 - Springer
... model, based on pseudorandom functions and **hash** functions, and (2 ... comes at a price: The secret **key** can only ... a κ-secure MMAC by **concatenating** many pseudorandom ...
Cited by 43 - Related articles - Web Search - BL Direct - All 10 versions

An Incremental Payment Method for Internet Based Streaming Real-Time Media
A Fuchsberger - Lecture notes in computer science, 1998 - Springer
... electronic schemes are based on public-**key** cryptography and ... T II s0, where 11 denotes **concatenation**, T is ... requiring more computation than a **hash** function, this ...
Related articles - Web Search - BL Direct - All 4 versions

Method and apparatus for cryptographic **key** establishment using an identity based symmetric keying ...
BJ Matt - US Patent App. 09/921,231, 2001 - Google Patents
... 410, decryptor 412, nonce generator 414, **hash** validator 416 ... KDCj is the identifier of **key** distri- bution ... generated by node 120, and II indicates **concatenation**. ...
Related articles - Web Search - All 4 versions

Authentication and payment in future mobile systems- ▶ kuleuven.be [PDF]
G Horn, B Preneel - Journal of Computer Security, 2000 - IOS Press
... and signs the **hash** value of the **concatenation** g s g ... in Section 3. U concate- nates the signed **hash** with his ... one session **key** K is derived from the master **key** g ...
Cited by 121 - Related articles - Web Search - BL Direct - All 21 versions

Exploration and synthesis of dynamic data sets in telecom network applications
C Ykman-Couvreur, J Lambrecht, D Verkest, F ... - Proceedings of the 12th international symposium on System ..., 1999 - portal.acm.org
... It supports **hashing** and **key** split- tingmerging, takes **key** ... specication, their size, their value **distribution**, the average ... in the table, and the **key** dependencies ...
Cited by 13 - Related articles - Web Search - All 8 versions

Paging during media loading
AH Maltz, JT Hurst, WE Elswick - US Patent App. 09/784,948, 2001 - Google Patents
... file can be done easily, by **concatenating** the contents ... asset encryp- tion and encryption **key** management preferably ... in three languages and two **video** formats, a ...
Cited by 1 - Related articles - Web Search - All 6 versions

[BOOK] Searching multimedia databases by content- ▶ psu.edu [PDF]
C Faloutsos - 1996 - books.google.com
... It starts from primary-**key** access methods, where B-trees and **hashing** are the ... dimensional time series, digitized voice or music, **video** clips, traditional ...
Cited by 237 - Related articles - Web Search - Library Search - All 4 versions

CNN algorithms for **video** authentication and copyright protection
M Csapodi, J Vandewalle, B Preneel - The Journal of VLSI Signal Processing, 1999 - Springer
... Authentication with Universal **Hash** Functions ... for authentication codes, however, each **key** can be ... provides no secrecy: the ciphertext is the **concatenation** of the ...
Cited by 1 - Related articles - Web Search - BL Direct - All 5 versions

The Internet—past, present and future
SP Sim, S Rudkin - BT Technology Journal, 1997 - Springer
... of names and is written by **concatenating** the hierarchy of ... correctly using the sender's public **key**, the claimed ... with the use of one-way **hash** functions, is the ...
Cited by 5 - Related articles - Web Search - BL Direct - All 7 versions

[PDF] Detection of image alterations using semi-fragile watermarks
ET Lin, CI Podilchuk, EJ Delp - PROC SPIE INT SOC OPT ENG, 2000 - Citeseer
... compression was hashed, the output of the **hash** function would ... the watermark image given the generator **key** and the ... Let T b * be the **concatenation** of the column ...
Cited by 109 - Related articles - View as HTML - Web Search - All 8 versions

Method and apparatus for establishing a shared cryptographic **key** between energy-limited nodes in a ...
DW Carman, BJ Matt - US Patent App. 09/887,585, 2001 - Google Patents
... indicates a **hash** code generated by **hash** code generator 322, KA is node **key** 306, NA ... generated by nonce generator 318, and | indicates **concatenation**. ...
Web Search - All 2 versions

Leveraging emerging network services to scale multimediaapplications- psu.edu [PDF]
K Calvert, J Griffioen, B Mullins, S Natarajan, L ... - Computer Communications and Networks, 2001. Proceedings. ..., 2001 - ieeexplore.ieee.org
... getTag(D): a tag extraction function returning a **hash** or **key** identifying the ... RTCP packet format already supports the ability to **concatenate** multiple RR ...
Cited by 3 - Related articles - Web Search - BL Direct - All 9 versions

Review of image and **video** indexing techniques
F Idris, S Panchanathan - Journal of Visual Communication and Image Representation, 1997 - Elsevier
... to represent the visual contents in textual form (eg, **key**- ... structures like B-tree and **hashing**, etc., cannot ... For **video**, the spatial features are generated using ...
Cited by 94 - Related articles - Web Search - BL Direct - All 5 versions

Method and apparatus for secure transmission of data and applications
G Karjoth, LJ O'connor - US Patent App. 09/748,446, 2000 - Google Patents
... such as a collection of public **key** certificates in a ... Instead, it employs a "linear" **hash** chain, such ... Several applications, such as **video** on-demand **distribution** ...
Web Search - All 2 versions

Fast and scalable layer four switching- ethz.ch [PDF]
V Srinivasan, G Varghese, S Suri, M Waldvogel - Proceedings of the ACM SIGCOMM'98 conference on Applications ..., 1998 - portal.acm.org
... the forwarding database of a router consists of a potentially large number of filters on **key** header fields. ... The first filter routes **video** traffic from SI to ...
Cited by 308 - Related articles - Web Search - All 18 versions

Method and apparatus to create encoded digital content
KL Milsted, KD Nguyen, Q Gong - US Patent 6,263,313, 2001 - Google Patents
... 1-37. S. Kent, "Privacy Enhancement or Internet Electronic Mail: Part II: Certificate-Based **Key** Management". RFC 1422, Feb., 1993, pp. 1-28. ...
Cited by 9 - Related articles - Web Search - All 2 versions

Digital watermarks: Shedding light on the invisible- informatika.org [PDF]
MM Yeung, BL Yeo, M Holliman - IEEE Micro, 1998 - ieeexplore.ieee.org
... 11 The technique **concatenates** the remaining high- order bits ... hashes them using a crypto- graphic **hash** function such ... then encrypted with a public **key**, XOR'ed ...

Cited by 6 - Related articles - Web Search - BL Direct - All 8 versions

[PDF] ▶ Robust audio watermarking using perceptual masking
MD Swanson, B Zhu, AH Tewfik, L Boney - Signal Processing, 1998 - Citeseer
... Most watermarking schemes focus on image and **video** copyright protection, eg, 1, 2, 3, 4, 5, 6 ... 3) are hashed to a **key** ... way **hash** functions may be used to compute ...
Cited by 300 - Related articles - View as HTML - Web Search - All 14 versions

Collusion-secure fingerprinting for digital data- ▶ nctu.edu.tw [PDF]
D Boneh, J Shaw - IEEE Transactions on Information Theory, 1998 - ieeexplore.ieee.org
... Marks have been embedded in digital **video** [6], [9], [10], [20], in documents [5], and in computer programs [12]. ... let where means **concatenation** of strings. ...
Cited by 682 - Related articles - Web Search - Library Search - BL Direct - All 11 versions

Security issues in a CDPD wireless network
Y Frankel, A Herzberg, PA Karger, H Krawczyk, CA ... - IEEE [see also IEEE Wireless Communications] Personal ..., 1995 - ieeexplore.ieee.org
... if employed) is either a **key distribution** center (in ... central entity sharing a distinct **key** with two ... MD5 with attached keysorblockcipher based **hash**- ing) that ...
Cited by 55 - Related articles - Web Search - All 11 versions

Multicast security and its extension to a mobile environment- ▶ kfupm.edu.sa [PDF]
L Gong, N Shacham - Wireless Networks, 1995 - Springer
... Moreover, the computation of a one-way **hash** function can be very ... Plaintext x encrypted under **key** k is denoted as {x}, and the **concatenation** of x and y ...
Cited by 47 - Related articles - Web Search - All 9 versions

A trusted process to digitally sign a document
B Balacheff, L Chen, D Plaquin, G Proudler - Proceedings of the 2001 workshop on New security paradigms, 2001 - portal.acm.org
... for example by the use of a **hash** function [10 ... image, since ii is encrypted under the TDC's public **key**. ... 3. The TDC signs the **concatenation** of the random number ...
Cited by 21 - Related articles - Web Search - Library Search - BL Direct - All 2 versions

The VersaKey framework: Versatile group **key** management- ▶ ethz.ch [PDF]
M Waldvogel, G Caronni, D Sun, N Weiler, B ... - IEEE Journal on selected areas in communications, 1999 - ieeexplore.ieee.org
... the nature of wide-scale **distribution** environments—the ... be discussed separately for each **key** management scheme ... eg, a cryptographically secure **hash**), then sends ...
Cited by 270 - Related articles - Web Search - BL Direct - All 27 versions

[PDF] ▶ Copy Detection Systems for Digital Documents
RD Smith - 1999 - pages.cs.wisc.edu
... produces the **distribution** of overlap that exists between overlapping documents, and it is ... Page 11. The **hash** values created are the **concatenation** of two ...
Cited by 2 - Related articles - View as HTML - Web Search - Library Search - All 3 versions

Method and system for providing a software license via the telephone
A Padole, E Wong, B Mehta - US Patent App. 09/792,608, 2001 - Google Patents
... 36 from the data derived from the product **key** and a ... [0031] The software product **concatenates** the product ID ... a **hashing** algorithm 112 to compute a **hash** value of ...
Web Search - All 2 versions

Broadcast encryption- ▶ psu.edu [PDF]
A Fiat - US Patent 5,592,552, 1997 - Google Patents

... a message (eg a **key** to decipher a **video** clip) to ... The levels refer to X sets of **hash** functions that ... **Key distribution** may be carried out as follows: the n users ...
Cited by 608 - Related articles - Web Search - BL Direct - All 14 versions

Computationally efficient method for trusted and dynamic digital objects dissemination
AD Narasimhalu, H Deng, W Wang - US Patent 6,058,383, 2000 - Google Patents
... of a pre-defined secure one-way **hash** function with ... By 52 is created in step 88 by **concatenating** the IP_Name 54 ... NSCO 66 is computed under the private **key** IPSK in ...
Cited by 5 - Related articles - Web Search - All 6 versions

Method and system for delivering encrypted content with associated geographical-based advertisements
MC Pelletier - US Patent App. 09/909,564, 2001 - Google Patents
Page 1. US 20030110130A1 (19) United States (12) Patent Application Publication (io> Pub. NO.: US 2003/0110130 Al Pelletier (43) Pub. Date: Jun. ...
Web Search - All 4 versions

Method and system for securing local database file of local content stored on end-user system
RL Spagna, T Zhao, DR Geisler, JC Mahlbacher - US Patent App. 09/884,618, 2001 - Google Patents
... in the trailer section then decrypting the reference table containing one or more data table location indicators for data items with the first decrypt- ing **key** ...
Web Search - All 4 versions

Attribute-based data dissemination for Internet applications- ▶psu.edu [PDF]
GR Malan, F Jahanian, S Subramanian - Journal of High Speed Networks, 1998 - IOS Press
... x. For example, x could denote the **concatenation** of 'Location ... forwarding graph using the tag-based **hash** table ... The use of text-based attribute **key**-value tuples ...
Cited by 4 - Related articles - Web Search - BL Direct - All 11 versions

Privacy and authentication on a portable communications system
MJ Beller, LF Chang, Y Yacobi, RB Bellcore - IEEE Journal on Selected Areas in Communications, 1993 - ieeexplore.ieee.org
... indicates the application of the D, operator or function to the **concatenation** of i and ... The two main public-**key** building blocks of our protocols are the Modular ...
Cited by 175 - Related articles - Web Search - BL Direct - All 5 versions

Digital content protection method and apparatus
PC Kocher, JM Jaffe, BC Jun - US Patent App. 09/948,473, 2001 - Google Patents
... short-lived subkeys from the main content decryption **key**. ... type is used in the "Divx" **video** playback system ... and algorithms used in content **distribution** systems. ...
Cited by 3 - Related articles - Web Search - All 4 versions

Software-efficient pseudorandom function and the use thereof for encryption
D Coppersmith, PW Rogaway - US Patent 5,454,039, 1995 - Google Patents
... A and B. The symbol "||" denotes the **concatenation** operator ... the **key** "a." In this particular example, the **key** is a ... may be derived from a secure **hash** algorithm, a ...
Cited by 31 - Related articles - Web Search - All 4 versions

System, method and article of manufacture for a payment gateway system architecture for processing ...
T Nguyen, DR Haller, MP Subramanian - US Patent 5,978,840, 1999 - Google Patents
... The gateway architecture includes three distinct sections to enhance **distribution** of the ... RK-4 ENCRYPT RK-4 WITH MERCHANT PUBLIC **KEY CONCATENATE** TRANSMIT -1250 ...
Cited by 10 - Related articles - Web Search - All 3 versions

[PS] ▶ Human and object tracking and verification in **video**
B Li - 2000 - umiacs.umd.edu
... It operates on monocular grayscale **video** imagery, or on **video** imagery from an infrared camera **...** j is the weight assigned to the j -th **distribution** of that pixel's **...**
Cited by 4 - Related articles - View as HTML - Web Search - Library Search

Pragma facility and SQL3 extension for optimal parallel UDF execution
F Carino Jr - US Patent 6,067,542, 2000 - Google Patents
... Data **Distribution** and Warehousing **...** BYNET RELATIONAL DATABASE SYSTEM J MULTIMEDIA OBJECT SERVER 504 J osc MANAGED NETWORKS (ATM, FDDI,...) **VIDEO**) OBJECT SERVER **...**
Cited by 17 - Related articles - Web Search - All 2 versions

System and method for accessing and storing data in a common network architecture
MC Driscoll, JT Cragin, SA Garcia, ML Galloway - US Patent App. 09/854,053, 2001 - Google Patents
... to, voice mail (audio and/or **video** data), electronic **...** sgarcia@edgemail.com [0030] The **hash** algorithm preferably **...** into a fixed-length value or **key** that represents **...**
Web Search - All 2 versions

A Unified PCA and DSP Based POD Module for Hybrid Cryptosystems
N Zhang - 2000 - nic-bnc.ca
... **hash** of data and then uses the private **key** to encrypt **...** In our project, the **hash** function SHA-1 is used **...** of the next-generation television and **video** systems has **...**
Related articles - Web Search - Library Search - All 2 versions

Method and apparatus for preventing piracy of digital content
PC Kocher, JM Jaffe, BC Jun - US Patent 6,289,455, 2001 - Google Patents
... for rather sophisticated and flexible **distribution** mechanisms. **...** lived subkeys from the main content decryption **key**. **...** is used in the "Divx" **video** playback system **...**
Cited by 6 - Related articles - Web Search - All 5 versions

Multicasting multimedia streams with active networks- ▶ berkeley.edu [PDF]
A Banchs, W Effelsberg, C Tschudin, V Turau - Local Computer Networks, 1998. LCN'98. Proceedings., 23rd ..., 1998 - ieeexplore.ieee.org
... self–chosen name (usually some random **key**): subsequent messengers **...** are DES and the MD5 **hash** function **...** simple values typically consists of **concatenating** the code **...**
Cited by 51 - Related articles - Web Search - BL Direct - All 26 versions

The Inferno™ operating system
SM Dorward, R Pike, DL Presotto, DM Ritchie, HW ... - Bell Labs Technical Journal, 1997 - interscience.wiley.com
... If it is not available, the **video**-decoder module is never **...** The signature covers a secure **hash** (SHA, MD4, or MD5 **...** of the party, the party's public **key**, and an **...**
Cited by 57 - Related articles - Web Search - BL Direct - All 2 versions

[PDF] ▶ 21 st Century's Hot Challenging Technologies in Telecommunications
P Dini, M Barbeau, M Lerner, I Stoica, R Popescu- ... - IEEE International Conference on Telecommunications (ICT ..., 2001 - Citeseer
... of the MD5 **hash** on the **concatenation** of the **...** The serial number facilitates re-**hashing** the same data **...** pervasive computing software, and review **key** open protocols. **...**
Cited by 1 - Related articles - View as HTML - Web Search - All 3 versions

Securing multimedia services over satellite ATM networks
H Cruickshank, I Mertzanis, BG Evans, H Leitold, R ... - International Journal of Satellite Communications, 1998 - interscience.wiley.com
... remote patient monitoring or operating theatre **video** conferencing. **...** with X's **key** K

X private **key** of X **...** X IdCert X X's certificate identifier **Hash**(text) one **...**
Cited by 1 - Related articles - Web Search - BL Direct - All 3 versions

[PDF] ▶ The design, implementation, and evaluation of cryptographic distributed applications: Secure PVM
N Venugopal - 1996 - Citeseer
... Various software mechanisms for message **hashing** and encryption are evaluated, including techniques for **key** generation and **key distribution**. **...**
Cited by 6 - Related articles - View as HTML - Web Search - Library Search

[PDF] ▶ Experimental Evaluation of FLIR ATR Approaches-A Comparative Study
B Li, R Chellappa, Q Zheng, S Der, N Nasrabadi, L ... - Computer Vision and Image Understanding, 2001 - cfar.umd.edu
... c 2001 Elsevier Science (USA) **Key** Words: automatic target **...** an nm-D vector is formed by **concatenating** its rows **...** such coordinate as an index to a **hash**-table, and **...**
Cited by 8 - Related articles - Web Search - BL Direct - All 11 versions

Programming Satan's computer- ▶ cmu.edu [PDF]
R Anderson, R Needham - Lecture Notes in Computer Science, 1995 - Springer
... a secret PIN; the calculator **concatenates** the challenge **...** mathematics of the underlying public **key** encryption algorithm **...** and if we ignore **hashing** (which makes no **...**
Cited by 143 - Related articles - Web Search - BL Direct - All 36 versions

[PDF] ▶ Epidemic routing for partially connected ad hoc networks
A Vahdat, D Becker - 2000 - Citeseer
... Thus, a **key** issue is determining whether to transmit **...** indicates which entries in their local **hash** tables are **...** This identifier is a **concatenation** of the host's **...**
Cited by 560 - Related articles - View as HTML - Web Search - All 19 versions

System for digitally signing a document
GJ Poudler, B Balacheff, L Chen, P It - 2000 - freepatentsonline.com
... the respective pixmap data, uses a **hash** algorithm to **...** FD, using the smartcard's public **key** (which it **...** the trusted display processor 260 **concatenates** the pixmap **...**
Related articles - Web Search - All 6 versions

External memory algorithms and data structures: Dealing with massive data- ▶ kfupm.edu.sa [PDF]
JS Vitter - ACM Computing Surveys (CSUR), 2001 - portal.acm.org
... the **key** paradigms include **distribution** and merging **...** Performance, Theory Additional **Key** Words and **...** block, B-tree, disk, dynamic, extendible **hashing**, external memory **...**
Cited by 423 - Related articles - Web Search - Library Search - BL Direct - All 21 versions

Computer readable device implementing a software-efficient pseudorandom function encryption
D Coppersmith, PW Rogaway - US Patent 5,675,652, 1997 - Google Patents
... The modification and **concatenation** steps are repeated to **...** this function for preprocessing (he encryption **key** into a **...** be derived from a secure **hash** algorithm, a **...**
Cited by 5 - Related articles - Web Search - All 2 versions

Key authors: **J Fridrich** - **R Wolfgang** - **E Delp** - **M Swanson** - **A Gionis**

Did you mean to search for: ***bash*** concatenate key video distribution

Gooogle ▶
Result Page: 1 2 3 **Next**

hash concatenate key video distribu Search

Google Home - About Google - About Google Scholar